SECURITY OPERATION CENTER – STUDY AND CAREER 2022

Joas Antonio

https://www.linkedin.com/in/joas-antonio-dos-santos/

SOC

- As a SOC analyst, your primary duty is to ensure that the organization's digital assets are secure and protected from unauthorized access. You protect both the online and on-premise infrastructures, monitor metrics and data to identify suspicious activity, and identify and mitigate risks before adversaries breach your system. Some adversaries will still breach your system, and a SOC analyst fights the frontline battle.

SOC TIER 1- KNOWLEDGEMENT

- Incidente Response – Procedures
- Malware Threats
- Command Line Basic (Linux)
- Sniffing and Filters TCPDump / Wireshark
- Log Analysis with SIEM or Log Manager (Graylog)
- Log Event Report, Collection and Correlactions
- Identifying attacks types
- Powershell Basics
- Identify Potential IoC
- Knowledgement Mitre Att&ck and Cyber Kill Chain

SOC TIER 1- RESPONSABILITIES

- Actively monitor and investigate security alerts to detect malicious activity
- Follow documented procedures to properly triage and respond to identified malicious activity, such as escalation or remediation actions
- Analyze data and events within the SIEM or SOAR for prioritization and priority elevation
- Communicate and collaborate with clients through the lifecycle of all escalated security investigations
- Participate in internal meetings, such as shift turn over, team meetings, etc. to collaborate with your fellow team members and perform knowledge transfer
- Stay up-to-date on the latest vulnerabilities, threats, and attacks around the world

SOC TIER 2 - KNOWLEDGEMENT

- SIEM Configuration and Administration
- Cyber Threat Intelligence
- Computer Forensic and Incident Response
- Incident Response Recovery
- Malware Analysis
- Identify Attack and Response
- Mitre Att&ck Applied
- Firewall, WAF, IDS, IPS and Others Solutions
- Runbooks and Playbooks
- Cloud (AWS, GCP, Azure)

SOC TIER 2- RESPONSABILITIES

- Create, develop and enhance SOC processes, runbooks and playbooks
- Perform investigation and escalations for complex or high severity security threats or incidents
- Monitor and investigate security events received through the SIEM or other security tools
- Provide recommendations for improvements to security policy, procedures, and architecture
- Supports/develops reports during and after incidents, which include all actions taken to properly mitigate, recover and return operations to normal operations.
- Conduct multi-step breach and investigative analysis to trace the dynamic activities associated with advanced threats

SOC TIER 3 - KNOWLEDGEMENT

- Cyber Threat Hunting
- OWASP Top 10
- Forensic Analysis Advanced
- Malware Analysis and Reverse Engineering Advanced
- Penetration Testing and Vulnerability Analysis
- Cyber Kill Chain and Mitre Att&ck
- Incident Response Advanced
- CIS Controls and Baseline Security
- Programming Language Skills
- Cloud (AWS, GCP, Azure)
- EndPoint Protection
- SIEM Management Advanced (Regex, Dashboards, Buildblocks and others)
- OSINT Techniques

SOC TIER 3 - RESPONSABILITIES

- Perform in-depth analysis of security events, including malware analysis, intrusion detection, all phases of security monitoring, and incident response
- Conduct initial evidence collection, case creation, and coordination/hand-off to other teams as necessary
- Respond in a timely manner (within documented SLA and Run Book) to support tickets.
- Contribute to SOC documentation such as standard operating procedures, playbooks, briefings and executive reports
- Participation in the Incident Response process
- Perform threat mitigation as required
- Participate in Red Team security preparedness evaluation exercises
- Actively hunt for Indicators of Compromise (IOC) and APT Tactics, Techniques, and Procedures (TTP) in the network and in the host as necessary

SOC – TIPS AND TRICKS

- Study security tools and solutions such as SIEM, SOAR, EDRs. You don't necessarily need to understand the administrative part, after all a Level 1 Analyst he only needs to have the knowledge at the beginning
- Understanding how the solutions work, if possible using a free-trial of the tool and taking a free course, helps to put you ahead in a selection process
- If the company requires knowledge in QRadar, download the community version, watch some video classes and do a basic PoC
- Certifications are also important, look for free certifications and invest too, as it will further elevate your professional curriculum
- Participate in workshops and events. Make labs to improve your skills, it will help you a lot

Labs:

https://www.linkedin.com/posts/joas-antonio-dos-santos_attack-defense-online-lab-activity-6981315732953272320-iH8G?utm_source=share&utm_medium=member_desktop

Certifications:

https://www.linkedin.com/posts/joas-antonio-dos-santos_cisco-certified-cyberops-associate-activity-6979479142245240832-FTz9?utm_source=share&utm_medium=member_desktop